常州市工业和信息化局文件

常工信信发〔2021〕97号

市工信局关于组织培育2021年度常州市工业信息安全防护星级企业的通知

各辖市、区工信（经发）局，常州经开区经发局：

为深入贯彻江苏省工信厅《江苏省加快推进工业互联网创新发展三年行动计划（2021—2023年）》（苏工信融合〔2020〕560号）《关于印发2021年全省信息化相关工作要点的通知》（苏工信信发〔2021〕60号），根据《关于深化“互联网+先进制造业”发展工业互联网的实施意见》（常政发〔2018〕115号）部署，经研究决定在全市开展2021年度工业信息安全防护星级企业培育工作。现将申报工作相关事宜通知如下：

一、申报条件

1.常州市范围内依法注册的规上工业企业；

2. 企业主要领导高度重视企业信息安全工作，对照《工业控制系统信息安全防护建设实施规范》（T/CESA1100-2020），已达到规划建设、单点防护阶段要求；

3. 企业经营状况良好，保持连续3年盈利；新注册企业具有良好盈利前景；

二、申报材料

常州市工业信息安全防护星级企业申报书纸质版、电子版。

三、有关要求

各辖市、区工信部门应高度重视，结合申报要求，积极组织本地区相关的行业龙头企业做好推荐申报。5月15日前，将申报材料(1份)报市工信局信息化发展处，联系电话：85681281。我市将对申报企业进行专家评审和现场核查后公布培育企业名单，并在培育企业中择优推荐申报升级工业信息安全防护星级企业。

附件：常州市工业信息安全防护星级企业申报书

常州市工业和信息化局

2021年3月29日

（此件依申请公开）

常州市工业和信息化局办公室　　2021年3月30日印发

附件

常州市工业信息
安全防护星级企业申报书

项目类别：工业信息安全类

申报单位：_____

联系人及手机：_____

填报日期：_____

常州市工业和信息化局印制

2021年3月

工业信息安全星级企业申报承诺书

申报单位	

申报单位承诺：

1. 本企业自愿向常州市工业和信息化局提出工业信息安全星级企业申报。

2. 本企业自愿遵守工业和信息化部、江苏省工信厅、常州市工信局工业信息安全相关文件规定。

3. 本企业自愿提供常州市工业和信息化局评审、管理、监督所需的数据资料，并为相关工作提供方便。

4. 本企业主要领导高度重视企业信息安全工作，能主动参与省、市工业信息安全相关工作。

5. 本申报材料所有内容真实有效，纸质申报材料与电子版申报材料一致。若出现问题，愿承担一切责任。

项目申报责任人：　　联系电话：

单位负责人：　　（单位公章）

日期：　　年　　月　　日

企业基本信息			
企业全称		统一社会信息代码	
法人代表		网络与信息安全分管领导	
企业名称		统一社会信用代码	
行业类别	*具体工业行业分类（见word文档）*	企业经济类型	*国有经济、集体经济、私营经济、个体经济、联营经济、股份制、外商投资、港澳台投资与其他*
企业地址	*具体到门牌号*	企业规模	*大型：500人以上* *中型：100-500人* *小型：50-100人*
企业简介	*1、企业主要业务；2、信息化建设、两化融合、智能制造等建设情况。*		
单位联系人		所属部门及职务	
电子邮箱		电话及手机号码	
信息安全专员		技术人员数量	
是否运营工业互联网平台	*若选择是，则填报内容增加工业互联网平台相关表单*	是否运营工业控制系统	*若选择是，则填报内容增加工业控制系统相关表单（DCS/SCADA等）*

互联网接入情况

是否连接互联网？ □是 □否 （如果连接互联网，请填写以下接入信息）			
域名（网址）		域名注册服务机构	
.cn域名的NS记录	*NS记录是指定由哪个DNS服务器解析你的域名*	.cn域名的A记录	*指定域名对应的IP地址*
IP地址范围			
主要协议/端口		操作系统及版本	
接入的运营商			
物理接入位置		接入带宽	
CDN IP地址范围		CDN服务提供商	

办公网络基本情况

办公网络运行的信息系统		
系统名称	系统功能简介	是否能从互联网访问
		□是 □否

办公网络硬件设备				
类别	名称	型号	数量	备注
服务器				
交换机/路由器				
路由器				
存储设备				

办公网络信息安全设备/系统				
类别	名称	型号/版本	数量	备注
防火墙				
入侵检测				
网络防病毒				
主机防病毒				
安全审计				
其他				

办公网络基础软件				
类别	名称	版本	数量（套）	备注
操作系统				
数据库				
中间件				
其他				

工业网络基本情况

工业网络运行的系统

类别	系统名称	功能描述	是否能从互联网访问
工业控制系统		*系统功能、业务流程，举例说明*	□是 □否
生产信息系统	*制造执行系统（MES）、ERP、工业云、其它*	*系统功能、是否国内品牌*	□是 □否
工业网络拓扑图	*工业网络拓扑简要示意图*		

工业网络软硬件设备

类型	类别	品牌（厂商）名称	型号	系统版本	数量
工业生产控制设备	可编程逻辑控制器（PLC）	*主要设备品牌厂商名称*			
	分布式控制系统（DCS）				
	远程终端设备				
	数控机床				
	工业机器人				
	智能仪表				
	其它				
工业网络通信设备	工业交换机				
	工业路由器				

	串口 服务器				
	其它				
工业主机设备	工业主机				
	组态软件&数据采集 与监控系统 （SCADA）软件				
	工业 数据库				
	其它				
工业网络安全设备	工业 防火墙				
	工业 网闸				
	主机安全防护设备				
	其它				

工业控制系统信息安全防护能力评估表

注：请对照评估内容，在评估结果处相应框中输入1

安全技术部分

控制族（13）	控制措施		防护要点	评估内容	评估结果		
					符合	部分符合	不符合
物理和环境安全（PE）	物理隔离保护（PE-1）	组织应对工业控制系统所在区域采取区域划分、物理隔离、访问控制、视频监控、专人值守等物理安全防护措施	组织应基于工业控制软硬件重要程度规划设立重点物理安全防护区域	是否已明确划分重点物理安全防护区域？			
			组织应对重点物理安全防护区域创建物理隔离保护管理文档	是否已有现行针对重点物理安全防护区域的物理隔离保护管理制度文档？			
			组织应基于重要工程师站、数据库、服务器、工业控制设备等核心工业控制软硬件划分重点物理安全防护区域	是否已针对核心工业控制软硬件（如：工程师站、数据库、服务器、工业控制设备等）划分重点物理安全防护区域？			
			在指定出入口采用围墙、门禁、门卫等物理访问控制措施，具有物理访问授权不代表对该区域工业控制系统组件有逻辑访问权	在物理安全防护区域出入口是否有物理安全访问控制措施（如：围墙、门禁、门卫等）？			
				人员物理访问授权与对应区域工业控制系统组件逻辑访问授权是否独立？			
			在物理访问工业控制系统设施前对人员的访问权限进行验证	是否在人员物理访问工业控制系统设施前，有对人员进行访问权限验证的操作？			
	应急电源（PE-2）	组织应为工业控制系统设立独立应急电源以保证其正常	组织中备有应急电源，能在紧急情况下为包括工业控制系统在内的设施提供电力保障	是否有能为工业控制系统提供电力保障的应急电源（可不只为工业控制系统供电）？			
			为工业控制系统配备应急UPS电源，并计算其续航时间	是否为工业控制系统配备应急UPS电源？ 若配备应急UPS电源，是否有续航时间测算记录？			
			提供短期不间断电源，以便在主电源失效的情况下正常关闭工业控制系统	是否为工业控制系统配备的短期不间断电源？			
	物理防灾（PE-3）	组织应具备物理防灾能力并部署相应防灾装置	组织应为工业控制系统创建物理防灾管理制度文档	是否有现行的工业控制系统的物理防灾管理制			
			为工业控制系统部署火灾检测和消防系统或设备，并维护该设备	是否已部署火灾检测和消防系统或设备？			
			应控制工业控制系统所在环境的温湿度，使其处于设备运行允许范围	是否对工控系统所在环境的温湿度进行测量记录，并判断是否符合要求？			
			组织应提供易用、工作正常的、关键人员知晓的总阀门或隔离阀门以保护工业控制系统免受漏水事故的损害	是否提供易用、工作正常、关键人员知晓的总阀门或隔离阀门以保护工控系统免受漏水事故的损			
通信网络安全（TN）	网络隔离（TN-	组织应分离工业控	组织应为开发和测试环境维护一个基线配置	是否为开发和测试环境维护基线配置？			
			组织应确保开发测试环境与实际生产环境物理相分离	开发测试环境是否与实际生产环境物理相分离？			
	区域划分（TN-2）	组织应对工业控制网络安全区域之间进行逻辑隔离安全防护	组织应建立安全区域划分策略	是否建立安全区域划分策略？			
			组织应根据区域重要性和业务需求对工业控制系统进行安全区域划分，以确保安全风险的区域隔离	是否根据区域重要性和业务需求合理划分工业控制系统进行安全区域？			
			组织应采用工业防火墙、网闸等防护设备，对工业控制网络安全区域实施隔离	是否采用工业防火墙、网闸等防护设备，对工业控制网络安全区域实施隔离？			
			组织应将具有相同功能和安全要求的控制设备划分到同一区域，区域之间执行管道通信，并对控制区域管道中的通信内容进行统一管理	控制设备是否按功能和安全要求划分到不同区域？ 区域之间是否执行管道通信，并对控制区域间管道中的通信内容进行统一管理？			
			组织可采用自动化机制，基于深度防御思想，智能生成区域访问控制策略并自适应演进，以针对不同安全区域的边界实现不同程度的安全隔离强度	网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件，是否能智能生成区域访问控制策略并自适应演进？			
	边界防护（TN-3）	组织应禁止没有防护的工业控制网络与互联网连接	组织应禁止未加防护的工业控制网络与互联网直接连接，确保互联网的安全风险不被引入工业控制网络	工业控制网络是否未发生在无防护状态下直接连接互联网的情况？			
			组织应在生产网和办公网边界部署安全防护设备，防止办公网的安全风险进入工业控制网络	是否在不同网络边界之间部署安全防护设备？			
			应能够对非授权设备私自连接到内部网络的行为进行限制或检查	是否在生产网和办公网边界部署安全防护设备，能够对非授权设备私自连接到内部网络和内部用			
			应能够对内部用户非授权联到外部网络的行为进行限制或	户非授权联到外部网络的行为进行限制或检查？			
			组织应监视并控制工业控制网络边界上的通信，以及网络内关键边界上的通信	工业控制网络边界的安全防护设备是否具有通信监控功能？			
	安全软件（IH-1）	组织应在工业主机中采用经过离线环境中充分验证测试的安全软件	应建立工业主机防病毒和恶意软件入侵管理制度，制定安全管理文档，确保该管理机制可有效防范防病毒和恶意软件入侵管理工作	是否建立工业控制系统防病毒和恶意软件入侵管理制度？			
			应在工业主机中安装安全软件，有效防护病毒、木马等恶意程序，防止未授权应用程序和服务运行	工业控制系统是否安装具备病毒、木马防护，未授权应用禁止等功能的安全防护软件？			
			安全软件应在离线环境中充分测试验证，确保其不会对工业控制系统的正常运行造成影响	安全软件是否已在离线环境中测试验证？			
			应依据采购合同、软件协议等规定的方式使用安全软件	是否按照采购合同、软件协议等规定的方式正确使用安全软件？			
			应定期对工业控制系统进行查杀，在临时接入设备使用前进行查杀，并做详细的查杀记录	是否定期对工业控制系统进行病毒查杀？ 临时接入设备使用前是否进行病毒查杀，并留存查杀记录？			
			组织应安装工业控制系统软件统一管理系统，以实现网络内工业主机安全防护软件的统一管理	是否安装工业控制系统安全软件统一管理系统？			
			工业主机上部署的安全软件，应能够及时识别网络入侵和恶意病毒，并及时告警	检测软件是否能够及时识别网络入侵和恶意病毒，并及时告警？			

工业主机安全（IH）	补丁升级（IH-2）	组织应密切关注重大工控安全漏洞及	应建立工业信息安全漏洞和补丁管理制度，确保组织掌握重大工业信息安全漏洞信息，并及时采取措施	是否建立工业信息安全漏洞和补丁管理制度？			
			出现重大工业信息安全漏洞后，应及时跟踪补丁发布，在适当时间（原则上不超过180天）进行补丁升级或开展消	出现重大工业信息安全漏洞时，是否及时进行补丁升级或消减措施？			
	外设管理（IH-3）	组织应拆除或封闭工业主机上不必要	应建立工业主机外设接口管理制度，严格管控工业主机外设接口的使用	是否建立工业主机外设接口管理制度？			
			应拆除或封闭工业主机上不必要的USB、光驱、无线等接口，防止病毒、木马、蠕虫等恶意代码入侵，并避免数据	是否拆除或封闭工业主机上不必要的USB、光驱、无线等接口？			
	身份认证（IH-4）	组织应在工业主机登录、应用服务资源访问等过程中采用身份认证措施	应建立身份认证管理制度	是否建立身份认证管理制度？			
			应建立密码口令管理制度	是否建立密码口令管理制度？			
			应根据不同业务需求、岗位职责等，合理分类设置账户	是否根据不同业务需求、岗位职责，合理分类设置账户？			
			应在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用身份认证管理技术（如口令密码、数字证书、生物指纹等）	在工业主机等登录访问过程中，是否使用了身份认证管理技术如口令密码、数字证书、生物指纹等）？			
			应明确禁止账户借用	是否明确禁止账户借用？			
			应以满足工作要求的最小特权原则来进行系统账户权限分	是否以最小特权原则来进行系统账户权限分配？			
			应为工业控制设备、工业通信设备等的登录账户设置高强度登录密码，并定期更新	账户是否设置高强度登录密码，并定期更新？			
			连续登录失败时，应限制账户的无效访问尝试	连续登录失败时，是否限制账户的无效访问？			
			应加强身份认证证书信息保护力度，禁止在不同系统和网络环境下共享 组织应确保其身份认证证书传输、存储的安全可靠，避免证书的未授权使用	是否加强对身份认证信息的保护力度，禁止在不同系统和网络环境下共享？			
应用程序安全（AP）	源代码审计（AP-1）	组织应开展工业控制系统应用程序的	组织制定相关管理制度，明确规定在部署运行应用程序前，应对其源代码进行安全性测试	企业信息安全保障相关文件，是否有针对工业控制系统的应用程序源代码进行安全审计的要求？			
			防止在工业控制系统相关应用程序中使用来自开源、受限制的或无认证源代码源的可执行代码	企业工业控制系统应用程序管理文件是否有禁止使用开源、受限制的或无认证源代码源的可执行			
	升级安全保障（AP-2）	组织应对工业控制系统应用程序进行安全升级	组织应针对应用程序的升级过程建立完善的安全保障制度	企业信息安全保障相关文件，是否有针对工业控制系统的应用程序制定升级过程安全保障的要			
			组织在对应用程序升级实施前，对升级包的来源进行可靠性验证	应用程序升级包是否通过官方渠道获得？ 是否有相应的检查工具，对升级包的签名或摘要值进行了检查确认？			
			组织应对应用程序升级后的运行情况进行持续跟踪，及时发现异常状况，确保系统稳定运行	是否对升级后的应用程序进行持续跟踪？ 是否有技术工具对升级后的异常状况进行发现和处理？			
数据安全防护（DP）	数据分类分级管理	组织应按照行业主管部门相	定期对工业数据资产进行分类梳理，建立工业数据资产目	是否建立工业数据资产目录？			
			应按照行业主管部门相关规定，开展工业数据分类分级工作	是否按照行业主管部门相关规定，开展工业数据分类分级工作，形成工作记录及分类分级结果？			
	数据备份（DP-3）	组织应定期备份关键业务数据	应建立关键数据清单（如生茶工艺、生产计划、组态文件、调度管理等数据）	是否建立关键业务数据清单（如生产工艺、生产计划、组态文件、调度管理等数据）？			
			应对关键数据实施本地定期备份，提供数据恢复功能	是否定期对关键业务数据实施本地备份？ 是否对关键业务数据提供数据恢复功能？			
			应对关键数据进行异地备份，利用受保护的通信网络将重要数据定时批量传送至备份场地	是否对关键业务数据进行异地备份？ 是否利用受保护的通信网络将重要数据定时批量传			
			应视企业业务需要，明确关键数据的备份方式、备份周期等策略，具备合理性，确保数据备份策略执行到位	是否根据业务需要，制定关键业务数据的备份方式、备份周期等策略，策略是否合理有效？			
			应定期对所备份的关键数据进行恢复测试，确保备份数据的可用性	是否定期对所备份的关键业务数据进行恢复测试，并形成测试记录；			
			应建立备份数据存储安全防护机制，采用数据加密、访问控制等手段，确保备份数据安全	是否对备份数据建立合理、有效的安全防护手段（如数据加密、访问控制等）？			
监测预警与态势感知（MS）	资产感知（MS-1）	组织应采取有效手段识别企业中工业控制系统、设备、平台等工业资产，监测资产安全运行状态，梳理企业资产清单	建立组织工业控制控制系统及安全重要资产清单	是否建立的工业控制系统及安全重要资产清单？ 工业控制系统及安全重要资产清单是否完整准确，覆盖组织研发、生产、测试环境中的工业控制系统、工业主机、制造装备、智能设备等，明确资产版本型号、运行状态、物理位置、联网情况等信息？			
	风险监测（MS-2）	组织应采取有效手段监测企业信息安全风险	应选择相关安全机构开展信息安全监测服务	是否选择具备一定资质的安全企事业单位，定期开展信息安全监测服务？ 是否签订监测服务合同，拟定监测服务方案？ 监测服务单位是否组织提供合理完备的监测服务及风险建议？			
			在工业控制网络部署网络安全监测设备，及时发现网络攻击或异常行为	是否在工业控制网络部署具备入侵检测、恶意病毒监测等功能的网络安全监测设备，及时发现网络攻击或异常行为并进行告警？			
			在重要工业控制网络中部署具备工业协议深度包检测功能的监测设备，审计违法操作	是否在重要工业控制网络中部署具备工业协议深度包检测功能的监测设备，审计违法操作并及时			
	威胁预警（MS-3）	应建立威胁预警机制，及时预警、处置企业可能存在的安全风险	应建立威胁预警机制	是否建立工控安全威胁预警机制？			
			及时关注国家级与省级工业信息安全风险预警平台发布的安全风险信息，按照安全建议采取风险消减措施	是否及时关注国家级与省级工业信息安全风险预警平台发布的安全风险信息？			
			及时将国家级与省级工业信息安全风险预警平台发布的重大安全风险通知到具体业务负责人，在企业内部开展针对重大安全风险的排查工作	对于重大安全风险是否及时通知到相关负责人，并按照安全建议采取风险消减措施？ 是否在企业内开展针对重大安全风险开展风险排查工作？			
小计					0	0	0

安全管理部分

控制面	控制项		控制要点	评估内容	评估结果		
					符合	部分符合	不符合
安全规划与机构建设（PD）	策略与规程（PD-1）	组织应建立工业控制系统的策略和规程	组织针对工业控制系统的信息安全制定了基本的制度文件，并明确规定由工业控制系统运维部门负责安全主体责任，牵头开展工业控制系统信息安全防护能力建设	企业是否有针对工业控制系统制定的信息安全制度性文件？ 企业部门职责划分制度文件是否由运维部门对工业控制系统负安全主体责任？			
			组织应制定并发布安全规划的策略，内容至少应包括：目的、范围、角色、责任、管理层承诺、相关部门间的协调和合规性	企业制定的策略与规程文件，是否包含目的、范围、角色、责任、管理层承诺、相关部门间的协调和合规性等内容？			
			制定并发布安全规划规程，以推动安全规划的策略及与相关安全控制的实施	企业是否在组织内部正式印发了安全规划规程等文件？			
	机构设置（PD-2）	组织应通过成立信息安全协调小组等方式，明确工控安全管理责任，落实工控安全责任制，部署工控安全防护措施	组织应建立工业控制系统信息安全管理机制，确保工控安全管理工作有序开展	是否建立工业控制系统信息安全管理机制？			
			组织应成立由组织负责人牵头，信息化、生产管理、设备管理等相关部门组成的信息安全协调小组，负责统筹协调工业控制系统信息安全相关工作	组织是否成立信息安全协调小组？ 协调小组成员是否包含信息化、生产管理、设备管理等相关部门？			
			各相关部门应在信息安全协调小组指导下，按照管理机制，明确工控安全管理责任人，落实工控安全责任制，部署工控安全防护措施	是否明确工控安全管理责任人及其职责？			
			组织应建立跨部门、跨职能的工业控制系统信息安全联合管理团队	是否建立跨部门、跨职能的工业控制系统信息安全联合管理团队？			
			制度执行应通过各相关部门协同落实	制度执行是否通过各相关部门协同落实？			
			组织联合产业链上下游，建立工业控制系统信息安全防护联合工作机制	是否联合产业链上下游，建立工业控制系统信息安全防护联合工作机制（工业信息安全防护联合工作协议等文件）？			
	职责划分（PD-3）	组织应明确各相关部门及工作岗位的职责	组织应设立信息安全管理工作的职能部门，专门负责工业控制系统信息安全相关工作	是否设立信息安全管理工作的职能部门，其工作职责是否明确？			
			组织应设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责	部门岗位职责文档，是否设立负责人岗位，并定义各负责人的职责？ 负责人岗位是否包括安全主管、安全管理等方			
			组织应设立系统管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责	组织是否明确各个工作岗位的职责？			
			根据需要建立适当的职责分离来消除在个人职责方面的利益冲突	组织是否根据需要建立适当的职责分离？			
			限制和控制特殊权限的分配和使用，根据用户的角色分配权限，实现用户的权限分离 如实现管理用户、操作系统特权用户的权限分离	组织是否根据用户角色分配权限，实现用户的权限分离？			
人员管理及培训（PT）	人员安全管理（PT-1）	组织应建立人员安全管理制度	应建立专门针对工业控制系统信息安全的人员安全管理制度，内容包需包括目的、范围、角色、责任、管理承诺等	是否建立针对工业控制系统信息安全的人员安全管理制度？			
			应定期对人员安全管理制度进行评审和更新	是否定期对人员安全管理制度进行评审和更新？			
			应建立工业信息安全岗位分类机制	是否建立工业信息安全岗位分类机制？			
			应建立人员审查制度，尤其对控制和管理工业控制系统关键岗位的人员进行审查	是否建立人员审查机制？ 是否定期对控制和管理工业控制系统关键岗位的人员进行审查？			
			在授权访问工业控制系统及相关信息前需进行人员审查	在授权访问工业控制系统及相关信息前，是否进行人员审查？			
			在人员离职或岗位调整时对其进行审查	在人员离职或岗位调整时，是否进行审查？			
			应终止离职人员对工业控制系统的访问权限	是否终止离职人员对工业控制系统的访问权限？			
			删除与离职人员相关的任何身份认证信息	是否删除与离职人员相关的任何身份认证信息？			
			与离职人员签订安全保密协议	是否与离职人员签订安全保密协议？			
			确保离职人员移交与工业控制系统相关资产和工具	是否监督离职人员移交与工业控制系统相关的资产和工具？			
			应保留所有工作人员（包括离职人员）的权限记录，发生重大安全事故时进行监视和审查	是否保留所有工作人员（包括离职人员）的权限记录？			
资产安全管理（AM）	设备资产管理（AM-1）	组织应建立和维护工业控制柜系统资产清单，明确资产管理责任人，以及	组织应制定设备资产管理制度	是否有现行的设备资产管理制度？			
			组织应建立工业控制系统资产清单（包括软件、硬件、固件等），确保工业控制系统资产信息可核查、可追溯	是否有在维护的工业控制系统资产清单（包括软件资产、硬件资产、固件资产等）？			
			组织应明确资产责任人并建立资产使用处置规则，以在资产生命周期内对其进行适当管理	是否有资产责任人列表？ 是否有现行的资产使用处置规则？ 是否有在维护中的资产生命周期管理日志记录？			
			应围绕组织工业控制系统承载的关键业务，制定涵盖关键主机设备、网络设备、控制组件等的重要资产清单	是否有为不同关键业务下的工业控制系统关键设备分别设立重要资产清单？			
	介质保护（AM-2）	组织应对使用的介质进行保护	组织应建立介质保护制度，包括介质登记、介质使用、介质销毁等，并定期对介质保护制度进行评审、更新	是否建立介质保护制度，是否包括介质登记、介质使用、介质销毁等？ 是否定期对介质保护制度进行评审和更新？			
			组织应对介质进行分类保护，将介质分为数字介质和非数字介质 其中，数字介质包括：硬盘、光盘、软盘、U盘等，非数字介质包括文档、微缩胶片等	组织的介质种类，是否进行分类保护？			
			受控区域内，应采取物理控制措施并安全存储各类介质，实行专人管理，并根据介质登记的清单定期盘点	受控区域内是否采取物理控制措施存储介质？ 介质存储环境是否由专人管理，并根据介质登记清单定期盘点？			
			受控区域外传递各类介质时，应采取安全防护措施进行保护和控制	在受控区域外传递介质时，是否采取安全防护措施？			
			在介质报废，回收前，应对介质进行销毁，采用销毁机制的强度、覆盖范围应与介质中存储信息的安全类别或级别相匹配	是否采用专业销毁技术对介质进行销毁？ 采用销毁机制的强度、覆盖范围是否与介质中信息的安全类别或级别相匹配？			

供应链安全（SC）	产品选型（SC-1）	组织应选择具有信息安全保障能力的信息技术产品和安全可控、利于维护的工业控制系统	组织应限制获取市场上具有安全能力的信息技术产品，在使用前应进行评估和确认	是否限制获取市场上具有安全能力的信息技术产品？ 信息技术产品的测试评估文档，组织在使用前是否进行评估和确认？			
	采购交付（SC-3）	组织应确保采购和交付过程的透明性和可控性	组织应在采购前建立与供应链信息安全风险承受能力相适应的采购策略，制定供应商的信息安全基线要求	产品采购策略，是否与供应链信息安全风险承受能力相适应？ 产品采购规范，是否制定供应商的信息安全基线要求？			
			组织应要求产品和服务供应商制定用户文档和使用指南，包括但不限于：产品和服务的安全配置、安装和运行说明、与管理功能相关的配置和使用方面的注意事项、对用户安全责任和注意事项的说明等	产品和服务的用户文档和使用指南，是否包括：产品和服务的安全配置、安装和运行说明、与管理功能有关的配置和使用方面的注意事项、对用户安全责任和注意事项的说明等？			
	合同协议控制（SC-4）	组织应与产品和服务供应商签订合同或协议，确保提供产品和服务的安全性	组织应与供应商签订产品和服务采购协议，并体现产品和服务安全保障、保密和验收准则等内容	是否与供应商签订产品和服务采购协议？ 采购协议中是否体现产品和服务安全保障、保密和验收准则等内容？			
			组织应以合同等方式明确工业控制系统产品和服务提供商承担的信息安全责任和义务，确保提供的产品和服务满足信息安全要求	与工业控制系统服务商签署的合同，是否约定服务商在服务过程中应承担的信息安全责任和义务？			
			针对工业控制系统设备提供商、集成商、工业企业、安全防护设备商、第三方测评机构等，以保密协议、合同等方式要求服务商做好保密工作，防范敏感信息外泄，并规定泄密后的后果	是否与工业控制系统设备提供商、集成商、工业企业、安全防护设备商、第三方测评机构等，签订保密协议？ 保密协议中是否明确保密内容、保密时限、违约			
			应在工业控制系统采购合同等法律文书中提出相关约束条款，明确不得安装隐蔽设备、模块或恶意软件，并在产品交收前进行验收检测判断产品质量是否符合供方需求	组织的工业控制系统采购合同等法律文书，是否明确不得安装隐蔽设备、模块或恶意软件？ 是否在产品交收前进行验收检测判断产品质量是否符合供方需求？（产品交付验收报告）			
应急响应（ER）	应急预案（ER-1）	组织应建立应急计划制度，制定应急预案	应建立应急计划制度，制定应急预案，包括目的、范围、角色、责任、管理承诺、组织实体之间的协调关系等	是否建立应急计划制度，制定应急预案？			
			应急预案中应识别工业控制系统业务应急需求、规定系统恢复优先级与目标、明确责任人	应急预案中是否根据工业控制系统应急需求，规定系统恢复优先级与目标、明确责任人？			
			应急预案中应包含：应急预案恢复计划、自动运行变更手动运行方案、应急响应者的角色和职责、应急响应者人员清单及联系信息等	应急预案中是否包含：应急预案恢复计划、自动运行变更手动运行方案、应急响应者的角色和职责、应急响应者人员清单及联系信息等？			
配置管理（CM）	安全配置（CM-1）	组织应建立工业控制系统安全配置清单，并定	组织应创建安全配置管理制度文档	是否有现行的安全配置管理制度文档？			
			组织应创建安全配置清单	是否有在维护的安全配置清单？			
			应对工业控制系统按照仅提供最小功能进行配置，对非必要功能、端口、协议和服务的使用进行禁止或限制	是否对工业控制系统按照仅提供最小功能进行配置，对非必要功能、端口、协议和服务的使用进行禁止或限制？			
	配置变更（CM-2）	组织应定义重大配置变更，进行重大配置变更时，应制定变更计	组织应设立配置变更日志文档管理制度	否有现行的配置变更日志文档管理制度？			
			组织应创建配置变更管理制度文档	是否有在维护的配置变更管理制度文档？			
			应定义重大配置变更（如重新划分网络等），在发生重大配置变更前，应制定配置变更计划，进行安全影响分析，确保该配置变更不会引入重大安全风险	是否有定义重大配置变更？ 是否有历史配置变更时制定的配置变更计划记录？			
			应确定配置变更类型，配置变更包括组件改变、技术产品的配置修改、紧急修改和缺陷修复等	配置日志文档是否有记录配置变更类型（如：组件改变、技术产品的配置修改、紧急修改和缺陷			
访问控制与审计（AA）	远程访问（AA-1）	组织应建立工业控制系统远程访问控制机制	组织应制定远程访问策略，原则上严格禁止工业控制系统面向互联网开通HTTP、FTP、Telnet等高风险通用网络服	是否制定了相应规章制度，禁止工业控制系统面向互联网开通HTTP、FTP、Telnet 等高风险通用			
			组织应采用数据单向访问控制等策略对远程访问进行安全加固，确保数据传输安全，避免未授权操作	针对远程访问安全控制策略，确认是否明确使用单向访问控制的安全策略？ 是否已通过有效的技术手段加以实现数据单向访问控制？			
			组织应对远程访问进行时限控制，并采用加标锁定策略，确保组织对远程访问的可控性	针对远程访问安全控制策略，确认是否明确对远程访问进行限时控制、加标锁定策略？ 是否已通过有效的技术手段加以实现远程访问限时控制、加标锁定策略？			
			适用时，组织应对远程维护采用虚拟专用网络（VPN）等远程接入方式，以确保远程维护安全可信	对远程维护是否采用虚拟专用网络（VPN）等远程接入方式？			
			组织应制定远程接入账户管理制度，规范账户申请、使用、收回等流程	是否建立远程接入账户管理制度，查阅其是否包含接入账户的申请、使用、收回（销毁）等流程			
	账户管理（AA-2）	组织应建立工业控制系统的账户管理机制	组织应制定账户管理的基本制度	是否制定了针对工业控制系统的账户管理相关规章制度？			
			组织应管理工业控制系统登入账户，包括建立、激活和修改、审核、禁用和删除账户	是否对工业控制系统的登入账户进行了统一管理？ 账户管理是否包括建立、激活和修改、审核、禁			
	口令保护（AA-3）	组织应建立工业控制系统的口令保护机制	组织应建立口令保护的基本制度	是否制定了针对工业控制系统的口令保护相关规章制度？			
			组织应根据工业控制系统的敏感程度，规定口令字符长度、组合复杂度、最小更新周期等参数	工业控制系统的口令保护相关规章制度，是否规范了口令的字符长度、组合复杂度、最小更新周			
			组织应妥善保存口令，严格控制口令知悉范围	工业控制系统的口令保护相关规章制度，是否规定了口令的知悉范围？			
			组织应要求产品或设备供应商告知系统存在的默认账户和口令，并及时进行修改；	供应商是否告知了系统默认账户和口令？ 工业控制设备、SCADA 软件、工业通信设备等是否对默认口令进行了修改？			
			组织应按规定的时间间隔更换访问控制设备的口令，在密码泄露和人员调动或离职时更换访问控制设备的口令	工业控制系统的口令保护相关规章制度，确认是否对口令更新间隔是否做出了规定？ 是否对密码泄露、人员调动或离职时需要更换口令做出规定？			
小计					0	0	0